Data Use And Non-Disclosure Agreement
Between
The New York City Department of Health and Mental Hygiene
And
The New York City Department of Homeless Services

This **DATA USE AND NON-DISCLOSURE AGREEMENT** ("Agreement"), effective on the date specified on the Signature Page ("Effective Date"), is hereby entered by and between the New York City Department of Homeless Services ("DHS" or "Data Owner"), having its primary offices at 33 Beaver Street, New York, NY 10004, and New York City Department of Health and Mental Hygiene ("DOHMH" or "Recipient"), having its primary offices at Gotham Center, 42-09 28th Street, Queens, NY 11101, (each a "Party" and, collectively, the "Parties").

WHEREAS, DHS provides temporary emergency shelter to New Yorkers experiencing homelessness; and

WHEREAS, DOHMH protects, improves, and promotes the health, productivity, and well-being of all New Yorkers; and

WHEREAS, DHS and DOHMH wish to collaborate to facilitate the provision of healthcare services to the thousands of migrants who recently arrived in New York City and currently living in DHS shelter facilities ("Migrants"); and

WHEREAS, DHS will share with DOHMH confidential information relating to DHS clients' names, date of birth, gender identity, CARES ID, and unit number at DHS facilities for purposes including, but not limited to, the provision of immunizations; tuberculosis detection, prevention and control; and prevention of other communicable diseases among Migrants; and

WHEREAS, pursuant to 45 CFR 205.50(a)(1)(i)(A), New York Social Services Law section 136 and Title 18 of the New York City Rules and Regulations sections 357.2(a) and 357.3(a), DHS is authorized to share Data, as defined herein, with DOHMH for purposes directly connected with the administration of public assistance; and

WHEREAS, the Parties desire to use the Data for public purposes that have been approved by DOHMH; and

NOW, THEREFORE, in consideration of the mutual promises and covenants contained in this Agreement, and other valuable and good consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree to the following:

I. TERM AND TERMINATION

A. **Term.** This Agreement shall commence as of the Effective Date and shall expire on June 30, 2025, unless terminated earlier pursuant to this Section I. The Parties may, upon mutual agreement in writing, extend this Agreement.

B. **Termination without Cause.** Any Party may terminate this Agreement at any time by providing thirty (30) days written notice to the other Party.

C. **Effect of Termination and Expiration.**

1. A Party that discloses data to another Party pursuant to this Agreement is a "Data Owner" of such disclosed data and a Party that receives data from another Party pursuant to this Agreement is a "Recipient" of such disclosed data herein. For purposes of this Agreement, DHS is the Data Owner and DOHMH the Recipient. Upon the expiration or termination of this Agreement for any reason, the confidentiality provisions set forth herein shall continue to apply to the Data shared with all Parties pursuant to this Agreement. Unless prohibited by law or otherwise agreed to by the Data Owner, upon expiration or termination of this Agreement for any reason, Recipient shall return all Data to the Data Owner that Recipient maintains in any form, and all copies of the Data in all its forms. Recipient shall not retain any Data thereafter. If requested by Data Owner, Recipient shall destroy all Data upon expiration or termination of this Agreement unless prohibited by law. Recipient must confirm in writing to Data Owner (using a form agreed upon by the Parties) the destruction of the Data, and all copies thereof by Recipient within sixty (60) days of the expiration or termination of this Agreement.

2. In the event that Recipient determines that returning or destroying all of the Data, and all copies of the Data, is infeasible or prohibited by law, Recipient shall provide to Data Owner notification of the conditions that make return or destruction infeasible or prohibited by law. Upon receipt of such notification, Recipient shall extend the protections of this Agreement to such Data and limit further uses and disclosures of such Data to those purposes that make the return or destruction infeasible or prohibited by law, for so long as Recipient maintains such Data.

II. PURPOSE OF AGREEMENT

A. This Agreement sets forth the terms and conditions under which Data Owner will transmit Data to Recipient and Recipient will use Data, as defined in Section III(A) of this Agreement. This Agreement also describes in **Attachment B** the uses of the data by Recipient. Furthermore, this Agreement also sets forth the security requirements that such access and use is conditioned upon, including the responsibilities the Parties agree to assume in connection with such access and use of the Data, and all permutations of the Data, and the procedures for security, transfer, use, retention, ownership, and confidentiality of the Data.

III. THE DATA

A. **Definition of Data.** "Data" means data maintained by DHS and provided to DOHMH pursuant to this Agreement and will include the data element set forth in **Attachment A**. All Data shall be Confidential Information.

B. **Identifying Information.** For purposes of this Agreement, "Identifying Information" shall have the meaning set forth in section 23-1201 of the New York City Administrative Code.

C. **Data Transmission.** Upon the execution of this Agreement by the Parties, DHS shall securely transmit Data to DOHMH by a secure method approved by the Parties. Such secure method may include but is not limited to encrypted email or secure file transfer protocol .

D. **Data Ownership.** DHS retains role ownership of Data. Recipient shall not make, cause to be made, use, or sell for any purpose any product or other item using, incorporating, or derived from the Data disclosed to Recipient, other than for the purpose stated in **Attachment B**. Data Owner may at any time request that the Data be promptly returned or destroyed by Recipient, unless determined to be infeasible or prohibited by law. Except as otherwise provided in this Agreement, upon written request by Data Owner, Recipient shall promptly return to Data Owner or destroy all Data, notes, and other tangible materials representing the Data and all copies and reproductions thereof (in whole or in part), and the Recipient shall not retain any Data thereafter. Where return or destruction is infeasible or prohibited by law, the Data retained shall be protected as provided in this Agreement.

IV. PERMITTED USES OF THE DATA

A. Recipient agrees to use Data solely for the purposes set forth in **Attachment B** to this Agreement, and for no other purposes.

B. To use Data for a purpose not authorized by this Agreement, Recipient shall request permission in writing from Data Owner. Only after obtaining written approval will such additional use(s) of Data be authorized.

V. LEGAL BASIS FOR DISCLOSURE

Pursuant to Section 136 of the New York State Social Services Law and Part 357 of the implementing regulations, public assistance records and information relating to a person receiving public assistance may be disclosed by a public welfare official to another agency when the disclosure is reasonably related to the purposes of the public welfare program and the function of the inquiring agency, the confidential character of the information will be maintained, and the information will not be used for commercial or political purposes. The implementing regulations provide enumerated legal exceptions to confidentiality that permit the disclosure of public assistance information, under limited circumstances. In

accordance with 18 NYCRR §357.2(a). DHS may disclose confidential public assistance data, to another agency DHS has determined is legally entitled to this data, for purposes directly connected to the administration of public assistance. According to federal regulation 45 CFR §205.50(a)(1)(i)(A), purposes directly connected with the administration of public assistance include establishing eligibility, determining the amount of assistance, and providing services for applicants and recipients. Here, DHS may disclose client identifiable public assistance information to DOHMH under this Agreement for purposes connected to the provision of health care and related services, including but not limited to helping immunize all school-aged children residing at DHS facilities in order to ensure these children meet immunization requirements to attend schools, as well as mitigation efforts to contain communicable diseases in DHS facilities housing Migrants.

Under New York City Administrative Code § 23-1202(b)(2)(a) and § 23-1202(c)(2)(a), the Agency Privacy Officer (APO) may in advance designate as routine certain collections and disclosures of Identifying Information between City Agencies when such collections and disclosures further the purpose or mission of the agency. The collections and disclosures of Identifying Information made by the Parties for the purposes set forth in this Agreement are covered by routine designations made by the DHS and DOHMH APOs in order to aid and inform the provision of public assistance, social services, public health interventions, and health care for homeless clients being served by either DHS and/or DOHMH.

VI. CONFIDENTIALITY AND SECURITY OF DATA

A. **Compliance with Applicable Privacy and Security Laws, Rules, and Regulations.** The Data provided under this Agreement shall be used and maintained in accordance with applicable provisions of federal, state, and local laws, rules, and regulations.

B. **Restrict Access to "Authorized Users".**

1. Access to the Data will be restricted to Recipient, Recipient's respective employees, agents and/or contractors required to use the Data to perform the activities of this Agreement that are set forth in **Attachment B**, and so designated as "Authorized Users" of Recipient.

2. Such Authorized Users must be notified and trained by Recipient as to the confidential nature of the Data and its proper handling.

3. Recipient certifies that all Authorized Users will be subject to the obligations of confidentiality and non-disclosure no less stringent than those contained in this Agreement.

4. Recipient shall maintain an up-to-date list of their Authorized Users and shall make the aforementioned list available to Data Owner upon request.

5. Recipient shall immediately notify Data Owner if any Authorized User has failed to comply with the terms of this Agreement and/or has compromised the privacy

and security of the Data. Such conduct may result in the immediate termination of Data access to that specific user.

C. **Privacy and Security.**

For Data disclosed to Recipient pursuant to this Agreement, Recipient shall be responsible for establishing and maintaining a data privacy and information security program ("Privacy and Security Program") that includes reasonable and appropriate physical, technical, administrative, and organizational safeguards, to: (a) ensure the security, confidentiality, availability, and integrity of Data; (b) protect against any anticipated threats or hazards to the security, confidentiality, availability, or integrity of Data; (c) protect against unauthorized or illegal or accidental disclosure, access to, destruction, alteration, modification, loss, acquisition or use of Data; (d) ensure the proper disposal of Data, if requested by Data Owner or required by applicable law; and, (e) ensure that all employees, agents, and contractors of Recipient comply with all of the foregoing. The Privacy and Security Program shall comply with the Citywide Privacy Protection Policies and Protocols of the New York City Chief Privacy Officer, available at https://www1.nyc.gov/site/moip/policy/the-policy.page. Except as otherwise provided in this Agreement, Recipient shall not, at any time, directly or indirectly, disclose, share, give, loan, sell, or otherwise grant access to the Data, in part or in whole, to any other person or organization.

D. **Security Incident.**

1. For the purposes of this Agreement, "Security Incident" shall mean an event that compromises the security, confidentiality, availability, or integrity of Data in the control of Recipient or its authorized users, including, but not limited to, by compromising the physical, technical, administrative, or organizational safeguards implemented by Recipient to protect the security, confidentiality, availability or integrity of Data disclosed to Recipient pursuant to this Agreement. Examples of a Security Incident include, but are not limited to, the unauthorized acquisition, use, access or disclosure of Data, intrusions, virus or malware, ransomware infections, social engineering, missing/stolen hardware, a breach of access credentials, distributed denial of service ("DDOS") and denial of service ("DoS") attacks.

2. Recipient shall implement, maintain, test, and update a Security Incident response plan. In the event of an actual or suspected Security Incident, Recipient shall:

   a. notify Data Owner within twenty-four (24) hours by written notice to the email addresses in the Notice section of this Agreement, summarizing, in reasonable detail, the nature and scope of the Security Incident (including a description of all impacted Data) and the corrective action already taken or planned by Recipient, which shall be timely supplemented to the level of detail reasonably requested by Data Owner, inclusive of relevant investigation or forensic reports;

b. promptly take all reasonable and necessary actions to confirm, contain and end the Security Incident, mitigate its impact to the Data and Data Owner, and prevent recurrence;

c. cooperate with Data Owner or its agents and other relevant City officials, including the City's Chief Privacy Officer, officials of the Department of Information Technology and Telecommunications, and the Office of Cyber Command, and officials of the Law Department in the investigation of the Security Incident, including promptly responding to the City's reasonable inquiries and providing prompt access to all evidentiary artifacts associated with or relevant to the Security Incident, such as relevant records, logs, files, data reporting, and other materials;

d. permit affected Data Owner, in its sole discretion, to immediately suspend or terminate Recipient's right to create, process, access, transfer, store, or dispose of Data;

e. not inform any third party that the Security Incident involves Data without first obtaining the other Party's prior written consent, except to the extent required by law or by third parties engaged by Data Owner or Recipient to remediate the Security Incident;

f. collaborate with Data Owner in determining whether to provide notice of the Security Incident to any person, governmental entity, the media, or other party, and the content of any such notice. Data Owner will make the final determination as to whether notice will be provided and to whom, the content of the notice, and which Party will be the signatory to the notice; and

g. promptly notify Data Owner of any investigations of data use, privacy or cybersecurity practices, or a Security Incident by a governmental, regulatory, or self-regulatory body.

VII. RECORD KEEPING

1. The Parties agree to retain copies of all their respective records related to this Agreement for a period of six (6) years after the termination of this Agreement. Federal, State and City auditors, and any other persons duly authorized by DHS or DOHMH, shall have full access to, and the right to, examine any of the said documents during said six (6) year period.

2. If this Agreement expires or is terminated for any reason, Recipient shall destroy all Data Owner's data in its possession or shall return such data to Data Owner, unless otherwise authorized in writing by Data Owner.

VIII. REQUIRED DISCLOSURE

In the event that the Recipient receives a court order, subpoena, other validly issued administrative or judicial notice or order, or request pursuant to applicable law ("legal process") to disclose the Data, prior to making such disclosure, Recipient shall, except where prohibited by law, notify Data Owner of such legal process as soon as practicable but in no event later than five (5) business days from receipt of such legal process, and provide Data Owner the opportunity to challenge or otherwise lawfully seek limits upon such disclosure of the Data.

IX. NOTICE

All notices under this Agreement shall be by email and shall be deemed delivered upon receipt. All notices shall be sent to email addresses set forth below. Each Party may change its contact information by notice to the other Parties; any such change shall take effect immediately upon delivery of such notice. Any notice pursuant to this Agreement shall be given or made to the respective Parties as follows:

For DOHMH:

New York City Department of
Health and Mental Hygiene
42-09 28th Street
Long Island City, New York 11101
Attn: Max William Hadler
Title: Director of Policy and Immigrant Initiatives
Email: mhadler@health.nyc.gov

For Security Incident Notifications
Cc: Nicholas Elcock, DOHMH Chief Privacy Officer
email: nelcock@health.nyc.gov

For DHS:

New York City Department of Homeless Services (DHS)
33 Beaver Street, 16th Floor
New York, NY 10004
Attn: Dr. Fabienne Laraque
Title: DHS Medical Director
Email: flaraque@dhs.nyc.gov

For Security Incident Notifications
Cc: Lauren Friedland, DSS/HRA/DHS Chief Data Privacy Officer
Email: friedlandl@dss.nyc.gov

X. PUBLICATION AND PUBLIC RELEASE OF DATA

Recipient shall not reveal any Identifying Information received pursuant to this Agreement, such as a person's first or last name, date of birth, or any other Identifying Information, in any draft or final publication, or publicly release such Identifying Information.

XI. MERGER CLAUSE

This Agreement and the Attachments hereto constitute the entire understanding of the Parties and merges all prior discussions, agreements, or understandings into it. No prior agreement, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or to bind any of the Parties.

XII. MODIFICATION

A. This Agreement may, from time to time, be modified by a writing signed by authorized representatives of the Parties. It may not be altered, modified, rescinded, or extended orally.

B. The Attachments hereto may be modified upon written agreement by the Parties without the need to formally amend this Agreement. Each attachment that is modified shall be deemed to be part of this Agreement and will supersede any prior Attachment, or Attachment modification, as applicable. Upon the modification of any Attachment, all references in this Agreement to such attachment shall be deemed to be references to the Attachment as modified.

XIII. NO THIRD-PARTY BENEFICIARY

Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties, any rights, remedies, obligations, or liabilities whatsoever.

XIV. ADDITIONAL PROVISIONS

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same Agreement. This Agreement may also be executed in counterpart facsimile or scanned signatures, each of which facsimile or scanned signature of a Party shall be deemed to be the original signature of such Party. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Parties to maintain the confidentiality and security of the Data. If any provision of this Agreement is found by a proper authority to be unenforceable or invalid, such unenforceability or invalidity shall not render this Agreement unenforceable or invalid as a whole and, in such event, such provision shall be changed and interpreted so as to best accomplish the objectives of such unenforceable or invalid provision within the limits of applicable law or applicable court decisions. Upon the expiration or earlier

termination of this Agreement, the continued use of Data for the purposes set forth in **Attachment B** shall cease. All other provisions of this Agreement shall survive.

IN WITNESS WHEREOF, and intending to be legally bound, the Parties hereto have executed this Agreement as of the day and date first written above.

NEW YORK CITY DEPARTMENT OF HEALTH AND MENTAL HYGIENE

By: _____
Celia Quinn, MD, MPH
Deputy Commissioner, Division of Disease Control

NEW YORK CITY DEPARTMENT OF HOMELESS SERVICES

By: Vincent Pullo Digitally signed by Vincent Pullo Date: 2023.12.05 11:54:59 -05'00'
Vincent Pullo
DSS ACCO

Data Use And Non-Disclosure Agreement

ATTACHMENT A – DATA POINTS

In accordance with Section III(A) of this Agreement, Data shall mean the data produced by DHS and transmitted via secure means to DOHMH, pursuant to this Agreement and will include, without limitation, the specific description and data elements set forth below:

DHS shall transmit to DOHMH the following categories of individual identifying information:

- **First Name**: Key Identifier
- **Middle Name**: Key Identifier
- **Last Name**: Key Identifier
- **Date of Birth**: Key Identifier
- **Gender Identity**: This identifying information is required to improve matching in systems including the Citywide Immunization Registry and the Electronic Clinical Laboratory Reporting System.
- **CARES ID**: This identifying information is required to facilitate matching between CARES and the Electronic Clinical Laboratory Reporting System to systematically identify DHS clients with existing TB test results and support coordination of follow-up.
- **Facility and Unit Number**: This identifying information is required to help with door-knocking efforts focusing on specific children who do not appear in the Citywide Immunization Registry.

Data Use And Non-Disclosure Agreement

ATTACHMENT B – PROJECT DESCRIPTION AND DATA USE

In accordance with Section IV(A) of this Agreement, DHS and DOHMH agree to use the Data solely for the purposes and project set forth below, and for no other purposes.

The purpose of disclosing the Data pursuant to this Agreement is to facilitate the provision of healthcare services to Migrants, including but not limited to immunizations; tuberculosis detection, prevention, and control; and prevention of other communicable diseases among Migrants. The sharing of Data shall be in furtherance of the vital goal of providing public assistance, social services, public health interventions, and health care to homeless individuals and families being served by either DHS and/or by DOHMH.

The purpose of this Agreement is to facilitate the disclosure of identifying information from DHS to DOHMH in furtherance of achieving goals related to the provision of healthcare services to Migrants residing at DHS facilities, including vaccination services and mitigation of communicable diseases in DHS facilities in which Migrants are residing. The information will not be used for commercial or political purposes.